BIOMETRIC TEMPLATE SECURITY USING HIGHER ORDER SPECTRA

Brenden Chen and Vinod Chandran

Queensland University of Technology, Brisbane, QLD, Australia

ABSTRACT

A method of improving the security of biometric templates which satisfies desirable properties such as (a) irreversibility of the template, (b) revocability and assignment of a new template to the same biometric input, (c) matching in the secure transformed domain is presented. It makes use of an iterative procedure based on the bispectrum that serves as an irreversible transformation for biometric features because signal phase is discarded each iteration. Unlike the usual hash function, this transformation preserves closeness in the transformed domain for similar biometric inputs. A number of such templates can be generated from the same input. These properties are illustrated using synthetic data and applied to images from the FRGC 3D database with Gabor features. Verification can be successfully performed using these secure templates with an EER of 5.85%

Index Terms— Face recognition, Higher order statistics

1. INTRODUCTION

Biometric template data must be protected to prevent information leakage in case of template compromise. Biometric data is inherently linked to an individual and can reveal **private** information about that individual such as their genealogy, personality and state of health [1]. The biometric itself (as opposed to a template) is permanent and therefore an individual can be cross-matched or tracked between two separate systems that use the same biometric modality. Furthermore, the feature extraction process of many biometric systems is invertible and template data can be used by an attacker to reverse engineer an artifact that can be used to spoof the system. For example knowledge of a trained PCA eigenspace coupled with the PCA eigenvalues for an individual allows reconstruction of the individual's face [2]. Fingerprint minutia information can also be reverse engineered from templates and used to create artificial fingerprints [3]. Template data is thus **insecure** and should be kept secret.

These issues raise a number of ethical, social and security problems that have hindered the uptake of biometrics and must be overcome if biometrics are to gain widespread acceptance. Template security techniques were first introduced in [4] and since then numerous other techniques have been proposed. Comprehensive reviews of the area are given in [5] and [6]. Existing techniques often fail to satisfy all three requirements: privacy, cancelability and security.

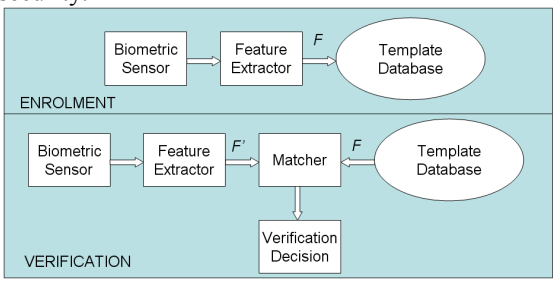

Figure 1. The enrolment and verification phases of a traditional biometric system. A person's biometric features (F) are extracted and stored during enrolment. Verification compares newly extracted features (F') with the stored template F.

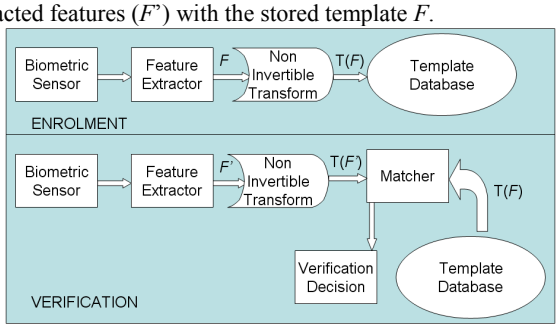

Figure 2. The enrolment and verification phase of the proposed secure biometric system. The persons biometric feature (F) is passed through a hash like function to produce a transformed copy T(F). Verification is done by comparing in the transformed (T) domain.

This paper proposes the use of a Higher Order Spectral (HOS) Transform that can be applied to biometric data as a secure hash function. This HOS transform is non-invertible, is robust to noise in the input allowing it to tolerate the natural variations present in a biometric and can be made to produce a large number of significantly different outputs given an identical input. A description of the HOS transformation is presented in section 2, followed by a demonstration of its desirable properties using synthetic data in section 3. We than apply the HOS transform to biometric features extracted from 3D facial images in the FRGC database in section 4 with a discussion and analysis of the results in section 5.

2. THE HIGHER ORDER SPECTRAL TRANSFORM

Most real world signals are not Gaussian in nature and cannot be fully described using only first and second-order moments (the mean and covariance). It is for this reason that Higher Order Spectra, which utilize higher than second-order statistics has been proposed for many signal processing applications [7]. Although originally defined for stationary and ergodic random signals, they have been extended to deterministic signals as well.

Of these higher than second-order statistics the third-order (the bispectrum) has proven to be the most popular due to its ease of computation. The bispectrum is the Fourier transform of the third-order moment and for a real valued deterministic signal $x(n)$ is given by:

$$B(f_1, f_2) = X(f_1)X(f_2)X^*(f_1 + f_2) \qquad (1)$$

The HOS transform described in this paper is based on the HOS feature extraction process introduced by Chandran and Elgar in [8, 9] which display a number of useful properties that make it a suitable template security scheme that satisfies all three requirements mentioned in the introduction.

1. The robustness to additive noise allows the HOS transform to tolerate small variations of the same biometric.
2. The bispectrum is complex-valued and discarding the phase information at each iteration allows for irreversibility.
3. The set of invariant HOS features described in [8] is sensitive to permutations while retaining robustness to small changes in amplitude or time scaling. This facilitates the design of a robust hash function.

The HOS transform is applied by taking the *N*-point discrete Fourier transform (DFT) of an amplitude and mean normalized version of the input signal $x(n)$ to obtain $X(f)$. Only the magnitude of $X(f)$ is retained, discarding the phase information prevents the inverse Fourier transform from being applied to obtain the original signal $x(n)$. This magnitude spectrum is the zero padded to length *N* and from this an estimate of the bispectrum can be extracted by Fourier transforming as in equation 1. The phase component of the bispectrum estimation $B(f_1, f_2)$ is retained that making it complex valued and sensitive to asymmetry.

Once the bispectrum is estimated HOS features can be extracted using the process proposed in [9]. The bispectrum is integrated along radial slices in the bifrequency plane to obtain:

$$V(a) = \int_{f_1=0+}^{1/(1+a)} B(f_1, af_1) af_1 \text{ where } a = \frac{1}{N}, \frac{2}{N}, ..., 1 \qquad (2)$$

Frequencies used in the above equation are first normalized by the Nyquist frequency and the zero frequency term (the average signal) is ignored. The variable a represents the slope of the line along which the integral of the bispectrum is computed.

The integrated bispectrum is then fed back as a complex valued input for the next iteration. The mean and amplitude normalization performed at the sat of each iteration ensures the output remains stable. After each iteration (*i*) a measure of change is taken between the current output and that of the previous iteration. This is in the form of a complex dot product (*D*) of the difference between the current ($V_i(a)$) and previous ($V_{i-1}(a)$) output with the previous output.

$$D_i(n) = \sum_{n=0}^{N-1} \left[V_{i-1}(a) - V_i(a) \right] * V_{i-1}(a) = M_i \exp(j\phi_i) \qquad (3)$$

The dot product between two complex vectors can be represented as a magnitude (M_i) and angle (ϕ_i) pair. The HOS transform will produce *i* such pairs, one for each iteration and can be visualized by plotting as a trajectory in polar coordinate space. The magnitude and angle pairs can be concatenated together to form the HOS transformed feature (*H*).

$$H = \left[M_1, M_2, .., M_i, \phi_1, \phi_2, .., \phi_i \right] \qquad (4)$$

Representing the output this way has a number of advantages. Firstly, the length of the output (*H*) is dependent solely on the number of iterations and not on the length of the original input. Secondly, H remains generic in appearance regardless of the nature of the input. The use for the dot product in producing D can be viewed as a second tier of information loss, this is because the integrated bispectra re not stored and cannot be calculated from *M* and ϕ.

3. THE PROPERTIES OF THE HOS TRANSFORM

In order to demonstrate the properties of the HOS transform that allow it to serve as a template security facilitator we show both the Gaussian noise immunity and the cancelability of the HOS features on a small test data set using artificial generated signals. A simple verification system based on the Mahalanobis distance classifier is used to distinguish between the three signals after the HOS transformation process. This verification system is trained using 15 slightly noisy (31dB SNR) versions of each of the original signals. The HOS transform is applied to each for 25 iterations and the expected value and standard deviations of the output feature vector are retained as training (template) data.

3.1 Gaussian Noise Immunity

Robustness of the output to input noise is an indication of how well the HOS transform will tolerate variations in the input feature vector that results from changes due to lighting and expression. Even the most invariant biometric modalities can display significant intra-class variation. This

will negatively impact verification performance in the HOS transformed feature space if no noise immunity is present.

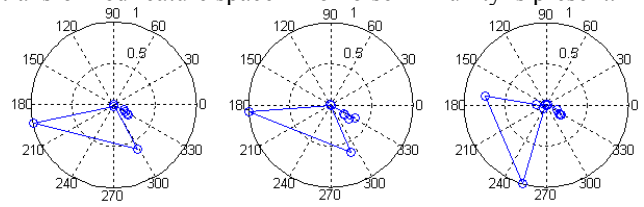

Figure 3. Trajectories of an identical input with different amounts of Gaussian noise. No noise, 30dB, 20dB.

By analyzing the HOS output trajectories of a noise free signal compared to the trajectories of those with different amounts of additive Gaussian noise it can be clearly seen that low levels do significantly affect the HOS output (Figure 3). It is only when the SNR degrades to 20dB before significant deviations in trajectory can be observed.

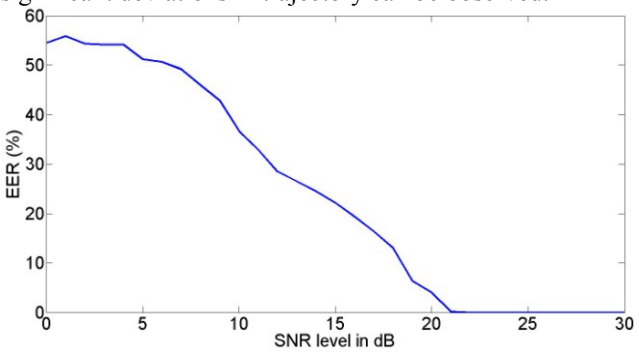

Figure 4. EER performance at different input noise levels.

These results are further demonstrated by attempting to classify using noisy inputs ranging from 30dB SNR to 0dB SNR. The EER obtained at each level is presented in Figure 4.

3.2 Cancelability

In order for a template security system to be cancelable it must be capable of producing different outputs given an identical input. The HOS transform, although robust to Gaussian noise, is still sensitive to permutations of the input. By applying different permutations different outputs can be obtained and since the process is one-way it is not possible for the original input to be recovered even if the permutation applied is known. It is this sensitivity combined with non-invertibility that allows cancelable templates to be produced.

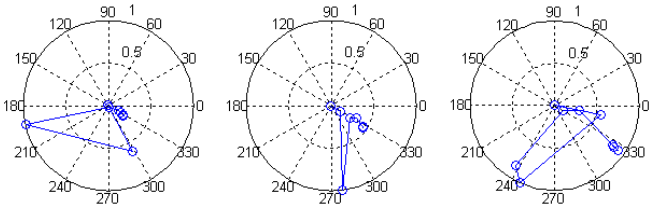

Figure 5. Original signal (left) compared against differently permuted versions of itself.

Given an input vector of length N there exists 2^N possible permutations. Even a small N of 10 gives 1024 possible combinations, more than enough template reissues for a life time in most applications. Figure 5 shows an original signal compared with 2 different permuted versions of it and shows the significant differences in trajectory caused by using a different permutation. This is further analyzed by producing 50 permuted versions of each signal and attempting to verify in the transformed domain. Figure 6 indicates that even at high SNR (low noise) only a poor EER of around 50% can be achieved. This will ensure that the new template will not be correlated to earlier ones.

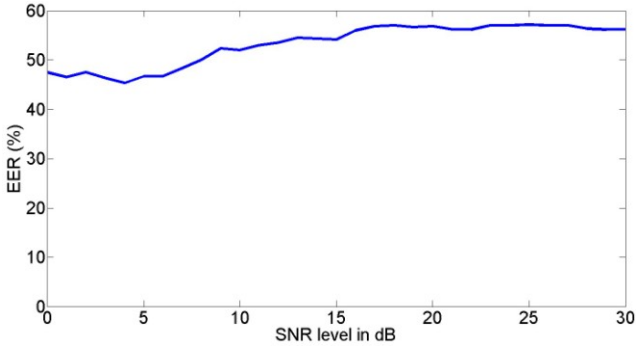

Figure 6. EER performance under different permutations and varying noise levels.

4. EXPERIMENTAL RESULTS

We apply the methodology to face recognition using the FRGC 3D database. The feature extraction is based on Elastic Bunch Graph Matching (EBGM) where Gabor jets are obtained at key fiducial points on the face. PCA is then applied to the Gabor jet features to remove redundancy and reduce dimensionality followed by LDA to maximize separation between classes. This is the baseline system whose output is then HOS transformed to produce secure templates.

The FRGC 3D database contains images for 298 individuals with between 4 and 30 images per person. In order to provide sufficient training and testing images per individual the 90 individuals who had less than 10 images were not included in the tests. Eight images from each of the remaining 208 individuals were used to train the system and the remainder (at least 2 per person) was used for testing.

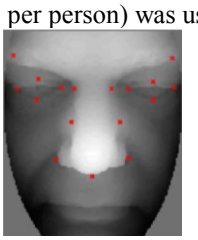

Figure 7. Sample images from the FRGC 3D database showing locations of the 17 fiducial points

The training images are manually landmarked to locate 17 fiducial points around the eyes and nose. At each point a

bank of 40 Gabor filters (5 frequencies at 8 rotations) are applied. The Gabor features from the training data is used to create the PCA (300 dimensions) and LDA (40 dimensions) spaces. When tested over the test data this baseline system can perform recognition at an EER of less than 0.01% (Figure 8).

This LDA feature vector is passed through the HOS transform to produce secure templates. These features are first zero padded to length 254 to improve spectral resolution in the frequency domain and HOS transformed for 25 iterations producing a length 50 output feature vector (*H*). A further step of PCA+LDA can be applied to improve discrimination of these transformed features. Experiments showed that the optimal number of eigenvectors retained is 40 for PCA and 10 for LDA achieving the best EER of 5.85% (Figure 8).

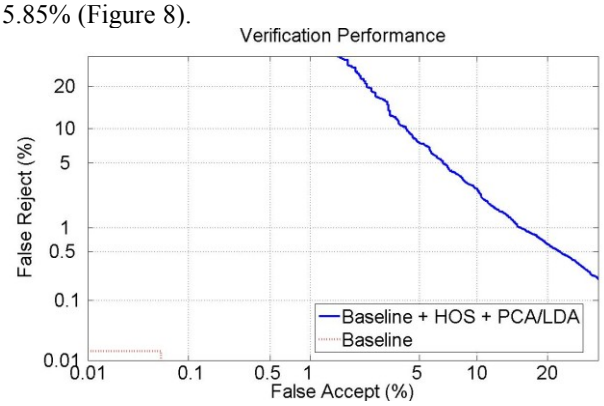

Figure 8. DET curves for baseline system and HOS transformed with PCA+LDA.

The overall system would require the storage of a number of parameters in the template, the PCA and LDA spaces first applied to the Gabor jet features, the permutation used prior to HOS transformation, the PCA and LDA spaces applied to H (output of the HOS transform) and the output of the final LDA step which is the final feature vector used for classification. From an attacker's perspective the loss of a user's template would allow reconstruction of *H* (using the final feature vector and the PCA/LDA spaces) since both PCA and LDA are invertible processes. However *H* cannot be inverted, preventing the attacker from gaining the original biometric input.

The process is also computationally feasible taking approximately 1.6 seconds on a Pentium Core 2 Duo 2.0 GHZ CPU to compute 25 iterations of the HOS transform for an input zero padded to length 256.

The added benefits of the HOS transform do come at a cost to verification performance. The use of a non-linear and unpredictable transformation makes it hard to prevent or limit this loss of discriminating information. However two keys points must be kept in mind. Firstly, although the baseline system has a good EER of near 0% it remains vulnerable to a number of attacks that rely on exploiting unprotected template data, the performance of such systems can degrade significantly when these attacks are carried out against them. Secondly, tests with synthetic data show that the amount of separability in the HOS transformed domain is directly related to the degree of separability in the input feature domain. If separation of classes can be improved and their intra-class variance minimized then performance in the HOS transformed domain would also improve. This could be achieved with improvements in feature extraction, multi-modal biometrics or new modalities such as DNA which is highly invariant and would benefit greatly from the added security benefits of the HOS transform

5. CONCLUSION

A new technique is proposed for producing secure biometric templates that guarantees security, privacy and cancelability. It uses a well known higher order signal processing technique in a novel application as a robust hash function that allows biometric template matching while preventing reconstruction of the biometric through inversion of template data.

6. REFERENCNES

[1] Y. Liu, "Identifying Legal Concerns in the Biometric Context," *Journal of International commercial Law and Technology* vol. 3, pp. 45-54, 2008.

[2] A. Adler, "Sample images can be independently restored from face recognition templates," in *Canadian Conference on Electrical and Computer Engineering*, 2003, pp. 1163-1166 vol.2.

[3] C. J. Hill, "Risk of masquerade arising from the storage of biometrics," Australian National University, 2001, p. 116.

[4] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal,* vol. 40, pp. 613-634, 2001.

[5] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Process,* vol. 2008, pp. 1-17, 2008.

[6] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE,* vol. 92, pp. 948-960, 2004.

[7] C. L. Nikias and J. M. Mendel, "Signal processing with higher-order spectra," *Signal Processing Magazine, IEEE,* vol. 10, pp. 10-37, 1993.

[8] V. Chandran, B. Carswell, B. Boashash, and S. A. Elgar, "Pattern recognition using invariants defined from higher order spectra: 2-D image inputs," *IEEE Transactions on Image Processing,* vol. 6, pp. 703-712, 1997.

[9] V. Chandran and S. L. Elgar, "Pattern Recognition Using Invariants Defined From Higher Order Spectra- One Dimensional Inputs," *IEEE Transactions on Signal Processing,* vol. 41, p. 205, 1993.